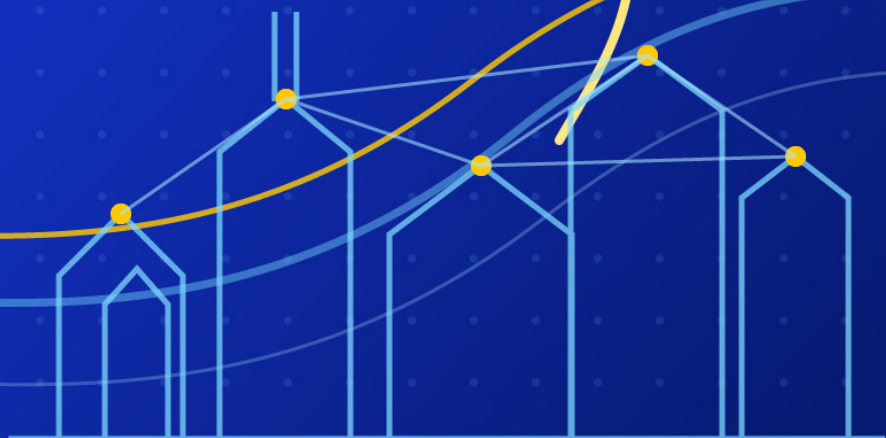
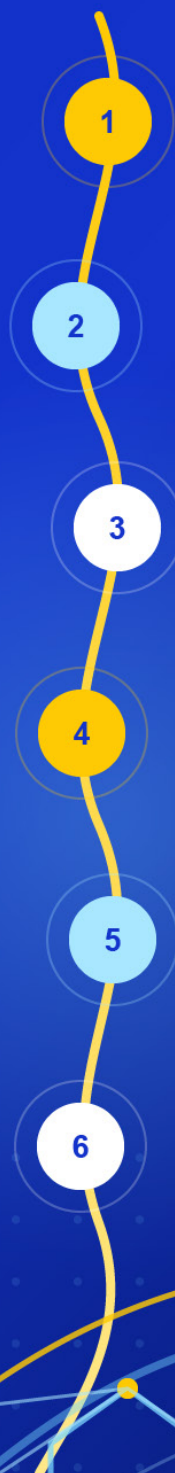




Singapore
2026 and Beyond

Security Roadmap

Visa Public



Executive summary

With technology evolving rapidly, businesses must adapt quickly to grow sustainably. This shift is about more than technology; it's about meeting the new expectations of digital-savvy consumers who seek personalised, convenient, and secure experiences. Companies must respond quickly to new trends and technologies, be it in data analytics or artificial intelligence (AI), by making strategic investments and ensuring their workforce is skilled to make the most of these tools.

In Singapore, 56.4% of firms in the financial and insurance sector have adopted AI, among the highest adoption rates across industries.²

While the democratisation of technology and most recently AI has benefited people and businesses, it has

also emboldened bad actors. Criminal activity in the digital domain has never been easier and more enticing than it is today. The consumerisation of cutting-edge technologies and the proliferation of new payment assets have spawned a new generation of cyber criminals, for whom hacking is now a side hustle.

The fraud and scam threat landscape has now evolved. The increased sophistication of cyberattacks, powered by AI and automation, continues to drive traditional unauthorised fraud through more damaging and targeted data breaches. However, there is also a significant shift from this unauthorised activity towards authorised payment scams. Fraud is adapting from technical compromise to behavioural manipulation, exploiting trust and urgency to deceive consumers.

The good news is that AI is also part of the solution. Visa has pioneered AI models in fraud protection since 1993, and today, our technology platform is among the most powerful examples of the tangible benefits of AI. Visa has over 150 AI and machine learning models in production, powering products that help solve longstanding challenges and pain points for consumers, merchants, and financial institutions.

The development and release of secure technologies, such as tokenisation and authentication have established a new foundation for digital payments security. This latest Visa Security Roadmap looks at the biggest challenges facing the payments ecosystem in the coming few years and the steps we can take together to minimise the impact on consumers, merchants, and other participants.

In this roadmap we will look at:

- Strengthening cybersecurity to anticipate emerging threats and enhance ecosystem resilience
- Advancing authentication for a seamless and secure digital experience
- Enabling safer transactions with tokenised payments
- Transforming eCommerce checkout to enhance consumer confidence and convenience
- Leveraging foundational standards to drive network performance
- Building a resilient payments ecosystem to combat fraud and scams in the AI era

Visa is committed to connecting the world through the most innovative, convenient, reliable, and secure payments network, protecting the payments ecosystem and facilitating global commerce for consumers, financial institutions, businesses, fintech partners, and government entities.¹

Our network spans:



MORE THAN

200+

COUNTRIES AND TERRITORIES



APPROXIMATELY

~14.5K

FINANCIAL INSTITUTIONS



MORE THAN

175M+

MERCHANT LOCATIONS



~5B

PAYMENT CREDENTIALS



US\$17T

IN TOTAL VOLUME



329B

TOTAL TRANSACTIONS
in its fiscal year 2025¹

¹ Visa Fact Sheet, Sep 2025, <https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/about-visa-factsheet.pdf>

² <https://www.mom.gov.sg/newsroom/press-releases/2026/0430-adoption-of-ai-among-firms>

The Journey

Since we first introduced our Singapore Security Roadmap in 2019 and the following edition in 2023, the payment landscape has transformed, bringing new conveniences along with a new generation of threats. The evolution from predictable fraud to sophisticated, AI-driven attacks and authorised payment scams demand a more dynamic defence.

In response, Visa has embedded advanced security technologies across the ecosystem. The following milestones represent the foundational journey we have taken to secure digital commerce:

Implement strong customer authentication



Singapore achieved full enablement of EMV® 3-D Secure across eligible issuing products, strengthening eCommerce authentication. Visa also partnered with acquirers to upgrade merchant terminals to EMV® chip acceptance, aligning with contactless specifications and reinforcing the infrastructure for secure, low-friction payments.

Drive adoption of secure technologies



Building on this foundation, Singapore introduced tokenisation to replace sensitive card data with secure tokens. This enhanced digital transaction safety, improved authorisation performance, and prepared the ecosystem for broader adoption as market and regulatory readiness evolved.

Enhance fraud prevention and detection with real-time risk scoring



Visa Singapore advanced fraud prevention by deploying real-time risk scoring powered by AI. This shift to dynamic, data-driven models enabled instant anomaly detection, reduced false positives, and reinforced regulatory alignment - elevating trust in digital payments.

Strengthen partner accountability with TPA registration and Visa Integrity Risk Program (VIRP) rollout



Visa Singapore aligned its third-party and merchant risk oversight. These changes clarified agent roles, improved merchant risk visibility, and enabled acquirers to manage compliance more efficiently supporting scalable, secure growth across the ecosystem.

Maintain compliance with Account Information Security (AIS) Program and PCI DSS v4



Singapore maintained strong compliance with Visa's AIS Program and transitioned to PCI DSS v4. Streamlined validation, proactive remediation, and third-party oversight strengthened data protection and reinforced ecosystem integrity.

A changing world

The COVID-19 pandemic pushed more consumers and businesses online in Singapore. With the increase in ICT technologies, Singapore's digital economy contributed nearly one-fifth to its economy in 2024, growing faster than overall GDP.³

Singapore's digital economy grew the fastest in Southeast Asia, clocking a compound annual growth rate (CAGR) of 12%, with growth expected to continue over the next few years.⁴

However, greater digitalisation and the growing use of AI have increased the threat posed by cyberattacks, scams and other forms of cyber-enabled fraud. In 2025, close to S\$1 billion was lost to scams. Although the number of reported scam cases declined by 27.6% to 37,308 and total losses decreased by 17.9% to approximately S\$913.1 million compared with 2024, the overall impact remains deeply concerning. Combating scams therefore remains a key priority for the government.⁵

Understanding the new threat landscape

As digital commerce accelerates, cybercriminals are evolving faster than ever, leveraging AI, automation, and global coordination to scale attacks. Visa's 2026 global threat intelligence highlights six critical trends reshaping the payments ecosystem. These insights are essential for Singapore's security roadmap as the region deepens its digital transformation.⁶



Scams Now Mirror Consumer behaviour in Real Time, with fraudsters targeting seasonal spending, tax refunds, and flash sales using fake offers and counterfeit promotions.



The Barrier to Becoming a Fraudster Has Hit an All-Time Low, as low-cost tools and automation make it easy for anyone to launch global scams from a mobile device.



AI-Powered Identity Attacks Are Accelerating. Deepfakes and synthetic IDs are now used to impersonate individuals and take over entire digital identities.



AI-Driven Scam Detection Is Becoming Core Infrastructure. Real-time AI

is mapping fraud patterns and disrupting scams before they spread across markets.



Investment⁵ and Romance Scams Are Growing Rapidly, exploiting delivery alerts and emotional trust to deceive victims and cause financial harm.



Real-Time Collaboration Has Become the Deciding Factor, with cross-border data sharing and industry coordination now essential to stop organised fraud.

³ Singapore Digital Economy Report 2025, <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/ar-sgde-2025>

⁴ Google, Temasek & Bain, "e Economy SEA report 2025: Southeast Asia's digital economy." <https://www.bain.com/about/media-center/press-releases/sea/e-economy-sea-2025/>

⁵ SPF, Annual Scam and Cybercrime Brief 2025, <https://www.scamshield.gov.sg/resources/scams-and-cybercrime-briefs/>

⁶ Visa, "6 Security Trends Shaping the Payments Ecosystem in 2026," January 2026, <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/6-security-trends-shaping-the-payments-ecosystem.html>

Navigating Singapore's Evolving Fraud Landscape

Fraudsters are adapting quickly. Attackers are using behavioural manipulation to exploit trust and urgency. In 2025, card-not-present (CNP) fraud represented the largest source of fraud losses in Singapore—reaching 16.2 basis points—versus an Asia-Pacific average of 11.7 basis points.⁷ Despite these challenges, the Anti-Scam Command (ASC) recovered over S\$140.5 million of scam losses in 2025, reflecting ongoing efforts by law enforcement and industry stakeholders to combat scams and strengthen consumer protection.⁸

GenAI is now being used to automate reconnaissance, customise scam narratives, and scale social engineering with precision. These developments are particularly relevant in Singapore, where investment, romance and government official impersonation scams (GOIS) have become increasingly sophisticated.

The rise in data breaches, which surged nearly 142% in 2025,⁹ continues to undermine Singapore's digital ecosystem as large-scale attacks grow more frequent and damaging. This reinforces the importance of cyber hygiene, incident response readiness, and secure merchant integration.



Visa Security Roadmap 2026 and Beyond

The latest edition of Visa's Security Roadmap outlines six focus areas to strengthen resilience in the payment ecosystem into 2026 and beyond.

- 1** Strengthening cybersecurity to anticipate emerging threats and enhance ecosystem resilience
- 2** Advancing authentication for a seamless and secure digital experience
- 3** Enabling safer transactions with tokenised payments
- 4** Transforming eCommerce checkout to enhance consumer confidence and convenience
- 5** Leveraging foundational standards to drive network performance
- 6** Building a resilient payments ecosystem to combat fraud and scams in the AI era

⁷ Visa, 12 months ending December 2025. Fraud rates are from issuing perspective.

⁸ SPF Annual & Cybercrime Brief 2025: <https://www.scamshield.gov.sg/resources/scams-and-cybercrime-briefs/>

⁹ The Straits Times, "Systems infected by malware in S'pore more than double in 2025: CSA," <https://www.straitstimes.com/tech/systems-infected-by-malware-in-spore-more-than-double-in-2025-csa>



1

Strengthening cybersecurity to anticipate emerging threats and enhance ecosystem resilience

In 2025, the Cyber Security Agency of Singapore (CSA) recorded 165 ransomware cases, a 4% year-on-year increase, alongside approximately 284,300 infected systems, up 142% from 2024,¹⁰ within Singapore's broader cyber threat landscape.

In response to rising cyber threats, Visa is actively enhancing its cybersecurity defences across the payment ecosystem.

Visa Network Defense (VND) delivers real-time, network-level fraud detection to stop large-scale attacks before they reach consumers. By analysing billions of transactions across ATM, CNP, and Point of Sales (POS) channels, VND detects anomalies and blocks threats instantly minimising losses, reducing regulatory risk, and protecting brand trust. It also offers actionable intelligence, 24/7 monitoring, and emergency support to strengthen the payment ecosystem.

Visa's Account Information Security Program (AIS) is a global compliance programme dedicated to maintaining the safety and integrity of the Visa payment ecosystem.¹¹ This is achieved through monitoring compliance and addressing security deficiencies to prevent compromise of Visa account data.

Payment Card Industry Data Security Standard (PCI DSS) compliance is mandatory for all entities storing, processing or transmitting Visa account data. PCI DSS provides the technical and operational requirements for financial institutions, merchants and service providers to protect against attacks aimed at stealing cardholder data.

Visa has transitioned to a more streamlined merchant PCI DSS compliance reporting approach. This shift is designed to help provide acquirers with greater control and autonomy in overseeing and managing their merchants' compliance with PCI DSS requirements. Visa will shift its focus to non-compliant merchant cases and will continue to work with acquirers that have merchants under remediation.¹¹

Part of Visa's consulting arm aids issuers in identifying system weaknesses through the Visa Payment Threats Lab (VPTL). This solution proactively detects potential vulnerabilities within payment systems, ideally before they are targeted by malicious actors. Typically, such security gaps only come to light following a fraudulent incident, but with VPTL, issuers can recognise and rectify gaps and vulnerabilities in advance.

2

Advancing authentication for a seamless and secure digital experience

Passkeys are a secure and convenient authentication method that uses biometrics or device-based cryptographic keys to replace passwords and SMS-based one-time passwords, both of which are often vulnerable to phishing and other social engineering attacks. Incorporating biometric authentication with tokenisation can greatly enhance the security of online transactions by ensuring consumers are accurately verified.

For merchants and acquirers, Visa introduced the Visa Secure minimum data requirements in August 2024, where merchants must provide required data in the authentication request.¹² A consistently high quantity and quality of data fields help enhance business outcomes for merchants, cardholders and issuers.



¹⁰ Cyber Security Agency of Singapore, Singapore Cyber Landscape 2025/2026: <https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2025-2026/>

¹¹ Visa, Account Information Security Program and PCI, accessed November 2024, <https://corporate.visa.com/en/resources/security-compliance.html#1>

¹² Visa, Payer Authentication Data Fields in Relation to Visa Secure Program Guide Updates, 17 September 2024, <https://support.visaacceptance.com/knowledgebase/knowledgearticle/?code=KA-04583>

3

Enabling safer transactions with tokenised payments

More than

1.9 Billion

tokens have been issued by Visa in the Asia Pacific region, supporting the growth in digital payments while enhancing security.¹³



5%

Authorisation Rate Lift¹³
Global Average for Visa Token CNP transactions



39%

Fraud Reduction¹⁴
Visa Token vs PAN-based CNP transactions

Tokenisation replaces a 16-digit debit or credit card number with a unique identifier, a token that only Visa can unlock. Visa tokens secure the payment credential, enabling the transfer of enhanced data, which can help improve payment success rates and lower fraud rates.

While tokenisation secures card data, its effectiveness depends on how tokens are provisioned. Fraud can occur when tokens are activated by bad actors, especially in device-bound wallets.

To combat this, we introduced Visa Provisioning Intelligence (VPI), an AI-based solution designed to combat token provisioning fraud at its source, which uses machine learning to rate the likelihood of fraud for token provisioning requests. VPI is designed to help reduce overall ecosystem fraud and increase the number of valid token provisioning requests.

4

Transforming eCommerce checkout to enhance consumer confidence and convenience

Digital payments are transforming how Singaporeans shop and transact and the checkout experience has become a critical point for both trust and conversion. Our latest innovations strengthen trust while making online and in-store payments faster, simpler, and safer.

One such innovation is Visa Click to Pay (CTP), built on EMV® Secure Remote Commerce (SRC) specifications. Click to Pay addresses checkout friction by reducing manual card entry and minimising exposure of sensitive card data through tokenisation and secure authentication. Consumers can complete transactions with fewer steps, without repeatedly

entering Primary Account Numbers (PANs) or card details across different merchants and devices.

Globally, we announced the launch of Visa Flexible Payment (Flex), expanding the eCommerce checkout experience by giving consumers greater control over how and when they pay. Flex enables cardholders to choose from eligible payment options such as instalments or deferred payments based on issuer-defined parameters and consumer preferences.

Together, Click to Pay and Visa Flexible Payment simplify the eCommerce checkout journey by reducing friction, minimising exposure of sensitive data, and enhancing consumer confidence.



¹³ VisaNet, January–December 2024. Visa credit and debit card-not-present transactions for tokenised versus non-tokenised credentials in the Asia-Pacific region. Authorisation rate is defined as approved authorisations divided by total authorisation attempts, based upon the first attempt of a unique transaction.

¹⁴ Visa Risk Datamart, Global, FY24 Q1–Q4 Token Fraud Rate versus PAN Fraud Rate by PV. Merchant rates may vary.

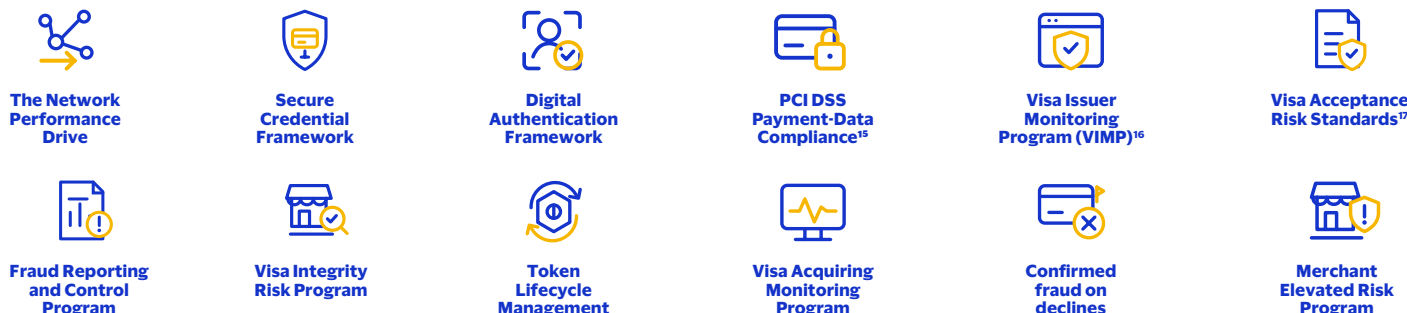


5

Leveraging foundational standards to drive network performance

Visa continues to enhance the integrity, security, and efficiency of the global payment system through a coordinated set of programmes and frameworks. These initiatives address every stage of the payment journey.

The following is a non-exhaustive list of programmes and updates that form the foundation of this effort:



6

Building a resilient payments ecosystem to combat fraud and scams in the AI era

In Singapore, it is more important than ever to stay ahead of evolving threats whether from cyberattacks, fraud, or scams. We have actively contributed to the development of key initiatives and solutions that support a safer digital ecosystem. Through continued investment in our technology and expertise, we are strengthening security, reducing fraud, and enabling seamless digital experiences for consumers and merchants across Singapore.

Globally, Visa has invested over US\$10 billion in technology and innovation over the past five years,¹⁸ further advancing our fraud prevention capabilities and reinforcing the security of our network.

In 2024, we expanded Visa Protect, a suite of risk and identity products designed to safeguard consumers and businesses with new AI-powered solutions aimed at reducing fraud for transactions both on and off Visa's network. These include account-to-account and card-not-present payments. Key solutions within the Visa Protect suite include:

- Visa Advanced Authorisation (VAA), which utilises machine learning to provide real-time risk assessments for transactions, helping identify and prevent fraud
- Visa Consumer Authentication Service (VCAS), which enhances security for online transactions by providing secure authentication methods such as biometrics

- Visa Provisioning Intelligence (VPI), which facilitates secure token provisioning to combat increasing token provisioning fraud
- Visa Account Attack Intelligence (VAAI) Score is a real-time risk score that uses AI and generative AI components to identify the likelihood of account enumeration attacks in card-not-present (CNP) transactions. It helps issuers detect and block compromised payment credentials before they are used for fraud.
- Visa Scam Disruption (VSD) complements these efforts by leveraging Visa's intelligence, analytics, and cross-ecosystem visibility to identify, investigate and disrupt scam networks before they can scale. By targeting scam enablers and supporting timely intervention, VSD strengthens Visa's ability to protect consumers and financial institutions from emerging scam threats.
- Visa Protect for Account to Account (VPAA), which offers additional protection for account-to-account transactions.

¹⁵ Visa, Account Information Security Program and PCI, accessed November 2024, <https://corporate.visa.com/en/resources/security-compliance.html#1>

¹⁶ Visa, Visa Core Rules and Visa Product and Service Rules, section 10.4.7.1, "Visa Issuer Monitoring Program (VIMP)," 18 April 2026, <https://corporate.visa.com/content/dam/VCOM/download/about-visa/visa-rules-public.pdf>

¹⁷ Visa, Visa Acceptance Risk Standards, 1 October 2024, <https://www.visa.com.sg/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf>

¹⁸ Visa, "Reimagining payments with Visa: Key trends shaping the future of 2025," <https://www.visa.com.ph/about-visa/newsroom/press-releases/reimagining-payments-with-visa-key-trends-shaping-the-future-of-2025.html>

Looking ahead

Visa will continue to engage our stakeholders and partners to meet the evolving needs of consumers and businesses, working together to secure the payment system in Singapore and globally.

Trust remains at the core of everything we do, and our collective responsibility is to continue to earn that trust by protecting individuals and businesses as the commerce landscape and threat environment evolves. Maintaining a secure payments ecosystem requires coordinated action across regulators, financial institutions, merchants, technology providers, consumers and payment networks, with every stakeholder playing a role in strengthening security and resilience. Together, we must drive security alongside payment innovation as we enable new and exciting ways to pay.

Considering these expectations of the Singapore threat landscape in the coming years, Visa has mapped the steps we are already taking with ecosystem partners during 2026 and into the coming years to highlight the critical areas for action.

2019



Implement strong customer authentication



Drive adoption of secure technologies



Enhance fraud prevention and detection with real-time risk scoring



Strengthen partner accountability with TPA registration and Visa Integrity Risk Program (VIRP) rollout



Maintain compliance with Account Information Security (AIS) Program and PCI DSS v4

2025



Accelerate adoption of secure, seamless payments with network token to boost approvals and reduce fraud



Detect and block large-scale fraud attacks and scams



Monitor fraud performance and reporting accuracy with VAMP and FRECOP



Strengthen merchant onboarding with updated Visa Acceptance Risk Standards (VARs) to block bad actors



Enhance consumer protection against scams

2026 and beyond



Conduct annual cyber posture assessments to ensure readiness



Shift from SMS OTP to biometric / in-app authentication, Visa Payment Passkeys and tokenisation to strengthen identity verification and reduce fraud



Streamline checkout through Click to Pay enablement to reduce card data exposure



Empower consumers with greater control

A photograph of a young couple sitting on a rooftop or balcony at night. The woman is holding a smartphone, and both are smiling and looking at the screen. The background shows a city skyline with lights.

Together, we navigate tomorrow with confidence enabling trust at every transaction and driving success across Singapore's digital economy.

For more information, please contact your Visa Risk Manager or visit visa.com/security